# M-3050/M-4050 Sensor Product Guide

Revision B

# McAfee® Network Security Platform

## COPYRIGHT

Copyright © 2014 McAfee, Inc., 2821 Mission College Boulevard, Santa Clara, CA 95054, 1.888.847.8766, www.intelsecurity.com

## TRADEMARK ATTRIBUTIONS

Intel and the Intel logo are registered trademarks of the Intel Corporation in the US and/or other countries. McAfee and the McAfee logo, McAfee Active Protection, McAfee DeepSAFE, ePolicy Orchestrator, McAfee ePO, McAfee EMM, McAfee Evader, Foundscore, Foundstone, Global Threat Intelligence, McAfee LiveSafe, Policy Lab, McAfee QuickClean, Safe Eyes, McAfee SECURE, McAfee Shredder, SiteAdvisor, McAfee Stinger, McAfee TechMaster, McAfee Total Protection, TrustedSource, VirusScan are registered trademarks or trademarks of McAfee, Inc. or its subsidiaries in the US and other countries. Other marks and brands may be claimed as the property of others.

## LICENSE INFORMATION

### License Agreement

NOTICE TO ALL USERS: CAREFULLY READ THE APPROPRIATE LEGAL AGREEMENT CORRESPONDING TO THE LICENSE YOU PURCHASED, WHICH SETS FORTH THE GENERAL TERMS AND CONDITIONS FOR THE USE OF THE LICENSED SOFTWARE. IF YOU DO NOT KNOW WHICH TYPE OF LICENSE YOU HAVE ACQUIRED, PLEASE CONSULT THE SALES AND OTHER RELATED LICENSE GRANT OR PURCHASE ORDER DOCUMENTS THAT ACCOMPANY YOUR SOFTWARE PACKAGING OR THAT YOU HAVE RECEIVED SEPARATELY AS PART OF THE PURCHASE (AS A BOOKLET, A FILE ON THE PRODUCT CD, OR A FILE AVAILABLE ON THE WEBSITE FROM WHICH YOU DOWNLOADED THE SOFTWARE PACKAGE). IF YOU DO NOT AGREE TO ALL OF THE TERMS SET FORTH IN THE AGREEMENT, DO NOT INSTALL THE SOFTWARE. IF APPLICABLE, YOU MAY RETURN THE PRODUCT TO MCAFEE OR THE PLACE OF PURCHASE FOR A FULL REFUND.

# Contents


**Preface** **5**

About this guide . . . . . 5

Audience . . . . . 5

Conventions . . . . . 5

What's in this guide . . . . . 6

Find product documentation . . . . . 6

**1 Overview** **7**

About Network Security Sensors . . . . . 7

Functions of a Sensor . . . . . 8

Network topology considerations . . . . . 8

M-3050/M-4050 key features . . . . . 9

M-3050/M-4050 physical description . . . . . 10

Ports . . . . . 10

Front and back panel LEDs . . . . . 11

**2 Before you install** **15**

Usage restrictions . . . . . 15

Safety measures . . . . . 15

About fiber-optic ports . . . . . 16

Contents of the box . . . . . 17

Unpack the Sensor . . . . . 17

**3 Setting up the Sensor** **19**

Setup overview . . . . . 19

How to position the Sensor . . . . . 19

Install the rails and ears on the chassis and rack . . . . . 20

Mount the Sensor on a rack . . . . . 20

Remove a Sensor from the rack . . . . . 20

Redundant power supply . . . . . 21

Install the power supply . . . . . 21

Remove the power supply . . . . . 22

Cable the Sensor . . . . . 22

Small form-factor pluggable modules . . . . . 23

SFP modules . . . . . 23

XFP modules . . . . . 24

Install a module . . . . . 24

Remove a module . . . . . 25

Power on the Sensor . . . . . 25

Power off the Sensor . . . . . 25

**4 Attaching Cables to the Sensor** **27**

Cable the Console port . . . . . 27

Cable the Auxiliary port . . . . . 28

Connect the cable to the Response port . . . . . 28

About the fail-open port . . . . . 29
Cable the Management port . . . . . 29
About connecting cables to the Monitoring ports . . . . . 29
How to use peer ports . . . . . 29
Default Monitoring port speed settings . . . . . 30
Cable types for routers, switches, hubs, and PCs . . . . . 30
Connect the cables for in-line mode . . . . . 30
Connect the cables for tap mode . . . . . 31
Connect the cables for SPAN or hub mode . . . . . 31
Cable the fail-over interconnection ports . . . . . 31
How does the fail-open function work . . . . . 32

**5 Troubleshooting the Sensor 35**

**6 Sensor technical specifications 37**

**A Regulatory, compliance, and safety information 39**

**Index 41**

# Preface

This guide provides the information you need to configure, use, and maintain your McAfee product.

**Contents**


- *About this guide*
- *Find product documentation*


## About this guide

This information describes the guide's target audience, the typographical conventions and icons used in this guide, and how the guide is organized.

### Audience

McAfee documentation is carefully researched and written for the target audience.

The information in this guide is intended primarily for:

- **Administrators** — People who implement and enforce the company's security program.
- **Users** — People who use the computer where the software is running and can access some or all of its features.

### Conventions

This guide uses these typographical conventions and icons.

| | |
|---|---|
| *Book title*, *term*, *emphasis* | Title of a book, chapter, or topic; a new term; emphasis. |
| **Bold** | Text that is strongly emphasized. |
| `User input, code, message` | Commands and other text that the user types; a code sample; a displayed message. |
| **Interface text** | Words from the product interface like options, menus, buttons, and dialog boxes. |
| Hypertext blue | A link to a topic or to an external website. |
| | **Note:** Additional information, like an alternate method of accessing an option. |

**Tip:** Suggestions and recommendations.

**Important/Caution:** Valuable advice to protect your computer system, software installation, network, business, or data.

**Warning:** Critical advice to prevent bodily harm when using a hardware product.

## What's in this guide

This guide contains information necessary to setup your M-3050/M-4050 Sensor model. This information includes guiding you through preconfiguring, cabling, and troubleshooting your Sensor.

# Find product documentation

McAfee provides the information you need during each phase of product implementation, from installation to daily use and troubleshooting. After a product is released, information about the product is entered into the McAfee online KnowledgeBase.

### Task

1 Go to the McAfee Technical Support ServicePortal at http://mysupport.mcafee.com.

2 Under **Self Service**, access the type of information you need:

| To access... | Do this... |
|---|---|
| User documentation | 1 Click **Product Documentation**.<br>2 Select a product, then select a version.<br>3 Select a product document. |
| KnowledgeBase | • Click **Search the KnowledgeBase** for answers to your product questions.<br>• Click **Browse the KnowledgeBase** for articles listed by product and version. |

1

# Overview

This chapter provides an overview of McAfee® Network Security Sensors in general and the M-3050/M-4050 Sensor model in particular.

**Contents**


- *About Network Security Sensors*
- *Functions of a Sensor*
- *Network topology considerations*
- *M-3050/M-4050 key features*
- *M-3050/M-4050 physical description*


## About Network Security Sensors

McAfee Network Security Sensors (Sensors) are high-performance, scalable, and flexible content processing appliances built for the accurate detection and prevention of:

- network intrusions
- network misuse
- Distributed Denial-of-Service (DDoS) attacks

Sensors are specifically designed to handle traffic at wire speed, efficiently inspect and detect intrusions with a high degree of accuracy, and flexible enough to adapt to the security needs of any enterprise environment. When deployed at key network access points, the Sensor provides real-time traffic monitoring to detect malicious activity and respond to the malicious activity as configured by the administrator.

After you deploy a Sensor successfully, you configure and manage it using the McAfee® Network Security Manager (Manager). The process of configuring a Sensor and establishing communication with the Manager is described in the subsequent chapters of this guide. For the details about the Manager, see the *McAfee Network Security Platform Getting Started Guide.*

# Functions of a Sensor

The primary function of a McAfee® Network Security Sensor (Sensor) is to analyze traffic on selected network segments and to respond when an attack is detected. The Sensor examines the header and data portion of every network packet, looking for patterns and behavior in the network traffic that indicate malicious activity. The Sensor examines packets according to user-configured policies, or rule sets, which determine what attacks to watch for, and how to respond with countermeasures if an attack is detected.

If an attack is detected, a Sensor responds according to its configured policy. Sensor can perform many types of attack responses, including generating alerts and packet logs, resetting TCP connections, "scrubbing" malicious packets, and even blocking attack packets entirely before they reach the intended target.

# Network topology considerations

Deployment of a Sensor requires knowledge of your network to help determine the level of configuration and the number of installed Sensors. You also need to determine the number of McAfee® ePolicy Orchestrator (McAfee ePO) /McAfee NAC servers required to protect your network. The Sensor is purpose-built for the monitoring of traffic across one or more network segments. For more information, see the *McAfee Network Security Platform Getting Started Guide.*

Following is an example of a network topology using Gigabit Ethernet throughput. In the illustration, McAfee® Network Security Platform (formerly McAfee® IntruShield®) provides IPS protection to outsourced servers. High port-density and virtualization provides a highly scalable solution, while Network Security Platform protects against Web and eCommerce mail server exploits.

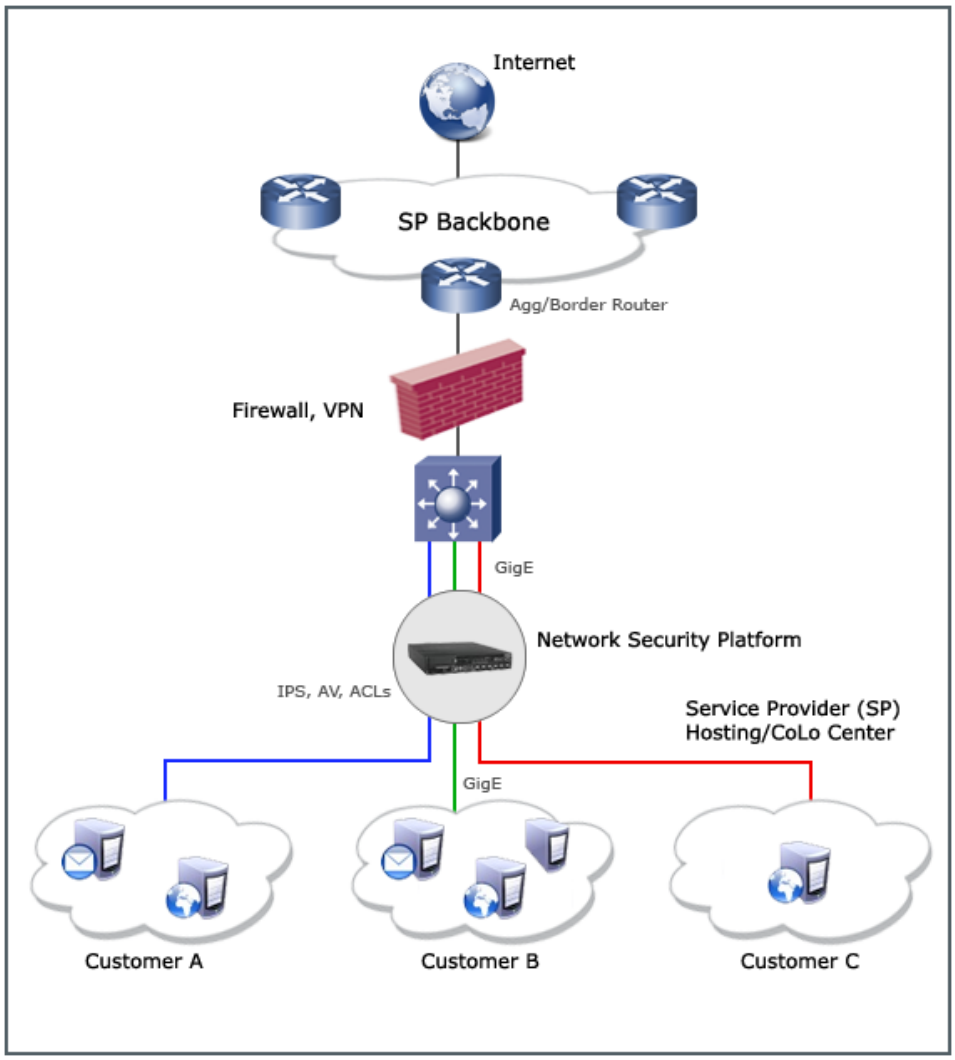


**Figure 1-1 A sample Network Security Platform deployment**

# M-3050/M-4050 key features

The M-3050/M-4050 Sensor includes the following features:

| M-3050 | M-4050 |
|---|---|
| 4 -10-GbE XFP | 4 -10-GbE XFP |
| 8 SFP ports (10/100/1000 copper or 1 GbE fiber) | 8 SFP ports (10/100/1000 copper or 1 GbE fiber) |
| 1 10/100/1000 Base-T Management port | 1 10/100/1000 Base-T Management port |
| 1 Response port | 1 Response port |
| Hot-swappable SFP/XFP modules | Hot-swappable SFP/XFP modules |

| M-3050 | M-4050 |
|---|---|
| Dual power supply | Dual power supply |
| 3 Fan units (that are field replaceable) | 3 Fan units (that are field replaceable) |
| It has 2 XLRs (A/B) host entries | It has 3 XLRs (A/B/C) host entries |
| Power slots for fail-open kit | Power slots for fail-open kit |

# M-3050/M-4050 physical description

The high-port density M-3050/M-4050, is designed for high bandwidth links, and is equipped to support two 10 Gigabit full-duplex Ethernet segments or four 10 Gigabit SPAN ports transmitting aggregated traffic. Additionally, it supports four 1 Gigabit full-duplex Ethernet segments or eight 1 Gigabit SPAN ports transmitting aggregated traffic.

## Ports

The M-3050/M-4050 is a 2RU (2 rack unit) and is equipped with the following components:

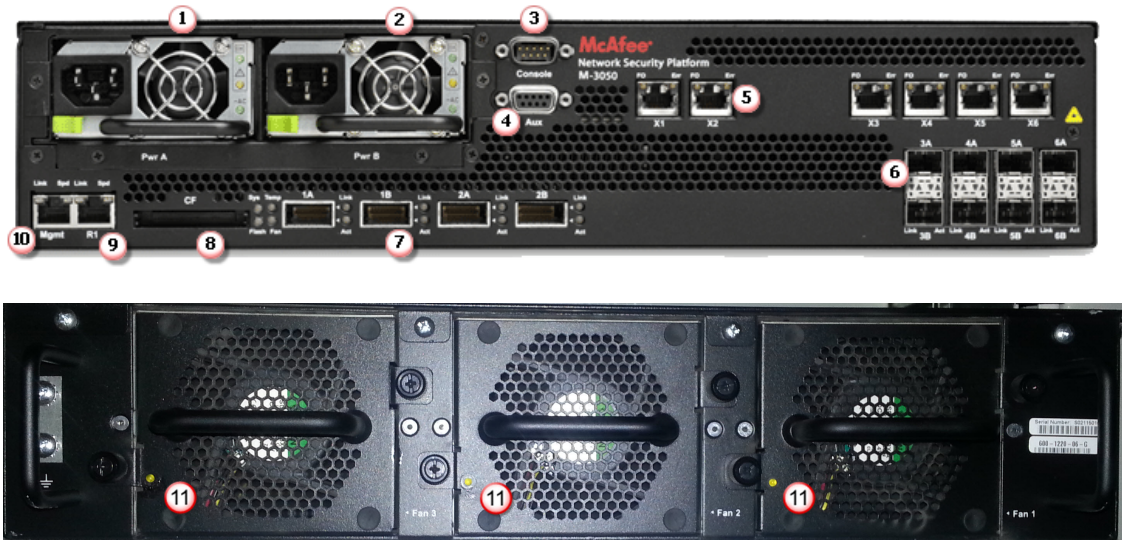


**Figure 1-2 An M-3050/M-4050 Sensor**

| Item | Description |
|---|---|
| 1 | Power Supply A |
| 2 | Power Supply B |
| 3 | RS-232C Console port |
| 4 | RS-232C Auxiliary port |
| 5 | RJ-11 Fail-Open Control ports |
| 6 | SFP Gigabit Ethernet Monitoring ports |
| 7 | XFP 10 Gigabit Ethernet Monitoring ports |
| 8 | Compact Flash port |
| 9 | RJ-45 Response port |

| Item | Description |
|---|---|
| 10 | 10/100/1000 Management port |
| 11 | Back panel LEDs (3) |

1 **Power Supply A.** Power supply A is included with each Sensor. The supply uses a standard IEC port (IEC320-C13). McAfee provides a standard, 2m NEMA 5-15P (US) power cable (3 wire). International customers must procure a country-appropriate power cable.

2 **Power Supply B** (optional, purchased separately). Power supply B is a hot-swappable, redundant power supply. This power supply also uses a standard IEC320-C13 port, and you can use McAfee-provided cable or acquire one that meets your specific needs.

3 **One RS-232C Console port**, which is used to set up and configure the Sensor.

4 **One RS-232C Auxiliary port**, which may be used to dial in remotely to set up and configure the Sensor.

5 **Six RJ-11 Fail-Open Control ports**, designed for use with the Optical Fail-Open Bypass kit. The ports are marked X1, X2, X3, X4, X5, X6, (1A-1B to 6A-6B respectively.)

6 **Eight small form-factor pluggable (SFP) 1 Gigabit Monitoring ports**, which enable you to monitor eight SPAN ports, four full-duplex tapped segments, four segments in-line, or a combination (that is, for example, two full-duplex segment and four SPAN ports).

7 **Four 10 Gigabit small form-factor pluggable (XFP) 10 Gigabit Monitoring ports**, which enable you to monitor four SPAN ports, two full-duplex tapped segments, two segments in-line, or a combination (that is, for example, one full-duplex segment and two SPAN ports).

The Monitoring interfaces of the M-3050/M-4050 work in stealth mode, meaning they have no IP address and are not visible on the monitored segment.

If you choose to run in failover mode, port 2A is used to interconnect with a standby Sensor.

The gigabit ports of the M-3050/M-4050 when deployed in in-line, fail-close, meaning that if the Sensor fails, it will interrupt/block data flow. Fail-open functionality requires either the Layer 2 Passthru feature or the hardware Gigabit Fail-Open Bypass kit for Gigabit ports. The Layer 2 Passthru feature is described in detail in the *McAfee Network Security Platform Device Administration Guide.*

8 **One External Compact Flash port**. This port is used only for flash recovery purposes. That is, this port is used in troubleshooting situations where the Sensor's internal flash is corrupted and you need to reboot the Sensor through the external compact flash. For more information, see the on-line KnowledgeBase at http://mysupport.mcafee.com/Eservice/. Click **Search the KnowledgeBase**.

9 **One RJ-45 Response port**, which, when you're operating in SPAN or tap mode, enables you to inject response packets back through a switch or router.

10 **One RJ-45 10/100/1000 Management port**, which is used for communication with the Manager server. You can assign an IP address to this port during installation.

The M-3050/M-4050 does not have internal taps; you must use it with a third-party external tap to run it in tap mode.

## Front and back panel LEDs

The front panel LEDs provide status information for the health of the Sensor and the activity on its ports. The following table describes the M-3050/M-4050 front panel LEDs.

| LED | Status | Description |
|---|---|---|
| Pwr A (Power A) | | |
| OK<br>⚠<br>~AC | Green<br>Amber<br>Green | Power Supply A is functioning.<br>Power Supply A is not functioning.<br>Power Supply in AC mode. |
| Pwr B (Power B) | | |
| OK<br>⚠<br>~AC | Green<br>Amber<br>Green | Power Supply B is functioning.<br>Power Supply B is not functioning.<br>Power Supply in AC mode. |
| ℹ If a power supply is not present, both green and amber LEDs are off. | | |
| Management Port Speed | Green<br>Amber<br>Off | The port speed is 1000 Mbps.<br>The port speed is 100 Mbps.<br>The port speed is 10 Mbps. |
| Management Port Link | Green<br>Off | The link is connected.<br>The link is disconnected. |
| Sys | Green<br>Amber | Sensor is operating.<br>Sensor is booting. (It could also indicate a system failure). |
| Fan | Green<br>Amber | All three fans are operating.<br>One or more of the fans has failed. |
| Temp | Green<br>Amber | Inlet air temperature measured inside chassis is normal. (Chassis temperature OK).<br>Inlet air temperature measured inside chassis is too hot. (Chassis temperature too hot). |
| Flash | Green<br>Off | Activity on external compact flash.<br>No activity on external compact flash. |
| Gigabit Ports (SFP / XFP) Act | Amber<br>Off | Data transferring.<br>No data transferring. |
| Gigabit Ports (SFP / XFP) Link | Green<br>Off | The link is connected.<br>The link is disconnected. |
| Response Port Speed | Green<br>Amber<br>Off | The port speed is 1000 Mbps.<br>The port speed is 100 Mbps.<br>The port speed is 10 Mbps. |
| Response Port Link | Green<br>Off | The link is connected.<br>The link is disconnected. |
| Fail-Open Control FO | Green<br>Off | The Sensor is providing power to the fail-open kit.<br>The Sensor is not providing power to the fail-open kit. |
| Fail-Open Control Port Err | Amber<br>Off | The fail-open control cable is disconnected or the Sensor is operating in bypass mode.<br>There is no error. |

The three back panel LEDs provide information regarding the Sensor fans.

| LED | Status | Description |
|---|---|---|
| Fan LED | OFF | The fan is functioning properly. |
| | Amber | The fan has malfunctioned. |

2

# Before you install

This chapter describes the best practices for deployment of Sensors in your network. Topics include the safety considerations for handling the Sensor, usage restrictions that apply to the Sensor model, and the contents that are shipped along with the Sensor.

**Contents**


- *Usage restrictions*
- *Safety measures*
- *About fiber-optic ports*
- *Contents of the box*
- *Unpack the Sensor*


## Usage restrictions

The following restrictions apply to the use and operation of a Sensor:

- You should not remove the outer shell of the Sensor. Doing so will invalidate your warranty.
- The Sensor appliance is not a general purpose workstation.
- McAfee prohibits the use of the Sensor appliance for anything other than operating Network Security Platform.
- McAfee prohibits the modification or installation of any hardware or software on the Sensor appliance that is not part of the normal operation of Network Security Platform.

## Safety measures

Please read the following warnings before you install the Sensor. These safety measures apply to all Sensor models unless otherwise noted. Failure to observe these safety warnings could result in serious physical injury.

**Warnings:**

- Read the installation instructions before you connect the system to its power source.
- To remove all power from the Sensor, unplug all power cords, including the redundant power cord.
- Only trained and qualified personnel should be allowed to install, replace, or service this equipment.
- Before working on the equipment that is connected to power lines, remove all jewelry including rings, necklaces, and watches. Metal objects will heat up when connected to power and ground, and can cause serious burns or weld the metal object to the terminals.
- This equipment is intended to be grounded. Ensure that the host is connected to earth ground during normal use.
- Do not remove the outer shell of the Sensor. Doing so will invalidate your warranty.
- Do not operate the system unless all cards, faceplates, front covers, and rear covers are in place. Blank faceplates and cover panels prevent exposure to hazardous voltages and currents inside the chassis, contain electromagnetic interference (EMI) that might disrupt other equipment and direct the flow of cooling air through the chassis.
- To avoid electric shock, do not connect safety extra-low voltage (SELV) circuits to telephone-network voltage (TNV) circuits. LAN ports contain SELV circuits, and WAN ports contain TNV circuits. Some LAN and WAN ports both use RJ-45 connectors. Use caution when connecting cables.
- This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy, and if not installed and used in accordance with the instruction manual, might cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case the users will be required to correct the interference at their own expense.
- Refer to the Appendix for information on regulatory, compliance, and other safety requirements.

# About fiber-optic ports

The Sensor uses fiber-optic connectors for its Monitoring ports. The connector type is a small form-factor pluggable (SFP) fiber optic connector that is LC-duplex compatible.

Note the following:

- Fiber-optic ports (for example, SFP/XFP, FDDI, OC-3, OC-12, OC-48, ATM, GBIC, and 100BaseFX) are considered Class 1 laser or Class 1 LED ports.
- These products have been tested and found to comply with Class 1 limits of IEC 60825-1, IEC 60825-2, EN 60825-1, EN 60825-2, and 21CFR1040.

To avoid exposure to radiation, do not stare into the aperture of a fiber-optic port. Invisible radiation could be emitted from the aperture of the port when no fiber cable is connected.

- Only FDA registered, EN 60825-1 and IEC 60825-1 certified Class 1 SFP laser transceivers are acceptable for use with the Sensor.

# Contents of the box

The following accessories are shipped in the Sensor box:

- One Sensor.
- One power supply.
- Two CD-ROMs containing the Sensor software and on-line documentation.
- Power cords. McAfee provides a standard and international power cables.
- One set of rack mounting rails.
- One set of rack mounting ears.
- One printed Slide Rail Assembly Procedure.
- One printed Quick Start Guide.
- Release Notes.

# Unpack the Sensor

### Task

1. Place the Sensor box as close to the installation site as possible.
2. Position the box with the text upright.
3. Open the top flaps of the box.
4. Remove the accessory box.
5. Verify you have received all parts.
   These parts are listed on the packing list and in the Contents of box section.
6. Pull out the packing material surrounding the Sensor.
7. Remove the Sensor from the anti-static bag.
8. Save the box and packing materials for later use in case you need to move or ship the Sensor.

**See also**

*Contents of the box* on page 17

# 3

# Setting up the Sensor

This chapter describes how to set up the Sensor for you to configure it.

**Contents**


- *Setup overview*
- *How to position the Sensor*
- *Redundant power supply*
- *Cable the Sensor*
- *Small form-factor pluggable modules*
- *Power on the Sensor*
- *Power off the Sensor*


## Setup overview

Setting up a Sensor involves the following steps:

1. Positioning the Sensor.
2. Installing interface modules (SFP and XFP).
3. Attaching power, network, and monitoring cables.
4. Powering on the Sensor.
5. Configuring the Sensor after you have set up and powered it on.

## How to position the Sensor

Place the Sensor in a physically secure location, close to the switches or routers it will be monitoring. Ideally, the Sensor should be located within a standard communications rack. To mount the Sensor on a rack, you will attach two mounting ears and rails to the Sensor as described in the subsequent sections of this guide.

**Tasks**


- *Install the rails and ears on the chassis and rack* on page 20

## Install the rails and ears on the chassis and rack

**Before you begin**

Before you install the rails and ears on the chassis, make sure that the power is *off.* Remove the power cable and all network interface cables from the Sensor.

Each rack-mounting rail and ear has holes that match up with holes in the chassis. You will need a screwdriver to secure the slotted panhead screws.

### Task

1 Verify that you have all the parts you will need — two three-in-one rails, two chassis ears, and fourteen slotted panhead screws.

Each rail includes a rail that mount to the rack, a rail that slides into the mounted rail, and a rail that is attached to the chassis.

2 Disassemble the slide rail by pulling the inner rail out and pushing the side latch in to separate.

3 Attach the inner rail to the chassis by fastening it with the screws provided.

4 Attach the ear to each side of the chassis.

5 Mount the L-shape and external rail to your rack frame.

The adjustable end of the L-shape rail is intended for placement at the back of your rack. Adjust the rail as needed for length. You are now ready to mount the Sensor on the rack.

## Mount the Sensor on a rack

McAfee recommends rack-mounting your Sensor. The rack-mounting hardware included with the Sensor is suitable for most 19-inch equipment racks and telco-type racks. For maintenance purposes, you must have access to the front and rear of the Sensor.

Before you mount the Sensor on the rack, make sure that the power is *off.* Remove the power cable and all network interface cables from the Sensor.

Due to the weight of the appliance, McAfee recommends that two people place the chassis into the rail cabinet.

Insert the chassis into the rail cabinet and complete the rack-mounting of the Sensor by securing the rack mount ears to two posts or mounting strips in the rack. The ears secure the Sensor to two rack posts. Make sure to fasten the ears securely to the rack.

Optionally, you can also mid-mount the Sensor. For details, refer to the corresponding Sensor *McAfee Network Security Platform Quick Start Guide.*

## Remove a Sensor from the rack

Review this section if you need to remove a Sensor from the rack.

Because of the weight of the appliance, McAfee recommends that two people remove the chassis from the rail cabinet. When removing the chassis from the rack, pull the chassis forward until you hear the innermost rails snap in place. On each side of the rails, press in the release button as pictured below and continue pulling the chassis.

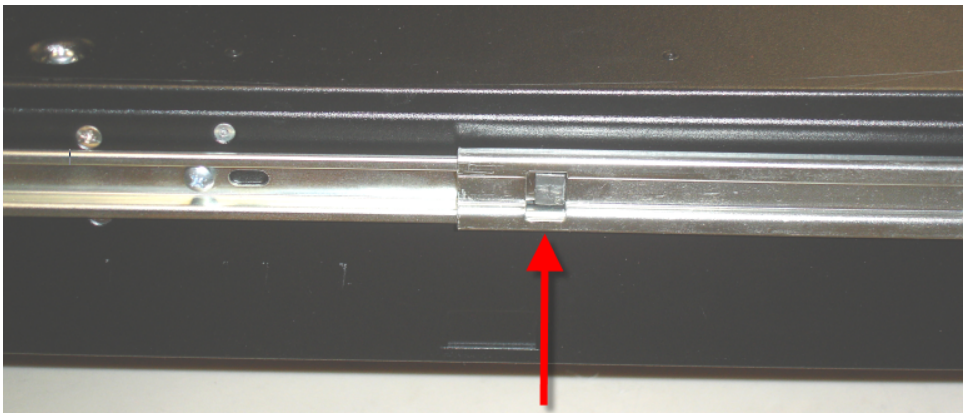

**Figure 3-1 Rail release latch**

# Redundant power supply

A basic configuration of the Sensor includes one hot-swappable supply. You can install a second hot-swappable power supply for redundancy. You will have to purchase this redundant power supply separately from McAfee. Each of these modules have one handle for insertion or extraction from the unit as well as a release latch.

**Figure 3-2 Power supply units**

## Install the power supply

### Task

1 Unpack the power supply from its shipping carton.

2 Remove the faceplate panel covering the power supply slot.

The faceplate panel must remain in place unless a power supply is in the power supply slot. Do not operate the Sensor without the faceplate panel in place.

3 Place the power supply in the slot with the cable outlet facing front and on the left side of the faceplate.

**Figure 3-3 Installing the power supply**

4 Slide in the power supply until it makes contact with the backplane, then push firmly to mate the connectors solidly with the backplane.

For true redundant operation with the optional redundant power supply, McAfee recommends that you plug each supply into a different power circuit. For optimal protection, use uninterruptable power sources.

## Remove the power supply

Note that the power supplies are hot-swappable. To avoid data interruption, do not power off both power supplies on an in-line Sensor, else the Sensor shuts down and all data traffic stops. Power off only the power supply you are replacing.

### Task

1 Unplug the power cable from its power source and remove the power cable from the power supply.

2 Put on an antistatic wrist or ankle strap.

3 Attach the strap to a bare metal surface of the chassis.

4 Push the release latch inward toward the handle.

5 Squeeze the handle of the power supply and pull it out.

6 Use faceplate panels to protect unused slots from dust and reduce electromagnetic radiation.

7 Replace the mounting bracket.

To remove all power from the Sensor, unplug all power cords.

# Cable the Sensor

Follow the steps outlined in Attaching Cables to the Sensor to connect cables to the monitoring, response, console, and management ports on your Sensor.

# Small form-factor pluggable modules

The Sensor uses two types of small form-factor pluggable modules as shown in the following table:

| Type | Performance |
|---|---|
| SFP | 10/100/1000 Mbps (copper)<br>1 Gbps (fiber optic) |
| XFP | 10 Gbps (fiber optic) |

Each module is a hot-swappable input/output device that plugs into an LC-type Gigabit Ethernet port, linking the module port with a copper or fiber-optic network. SFP optical interfaces are less than half the size of GBIC interfaces.

To ensure compatibility, McAfee supports only those SFP and XFP modules purchased through McAfee or from a McAfee-approved vendor. For a list of approved vendors, locate the relevant KnowledgeBase article at http://mysupport.mcafee.com/Eservice/. Click **Search the KnowledgeBase**.

These installation instructions provide information for installing SFP and XFP modules that use a bail clasp for securing the module in place in the Sensor. Your module might be slightly different. Check the module manufacturer's installation instructions for more details. For ease of installation, insert the module in the Sensor while it is powered down and before placing it on a rack.

To prevent eye damage, do not stare into open laser apertures.

## SFP modules

An SFP module is a hot-swappable, protocol-independant, compact, optical receiver, which allows for greater port density than the standard GBIC. This module operates at varying speeds for up to 1 gigabit per second on SONET/SDH, Fibre Channel, Gigabit Ethernet and other applications. An SFP module operates in single mode and multimode. Additionally, this module transmits on a 850-nanometer wavelength on short reach (SR) and 1310-nanometer wavelength on long reach (LR).

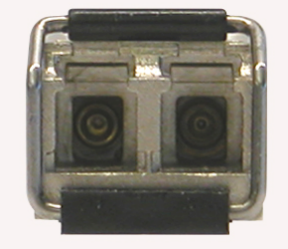

**Figure 3-4 An SFP module**

## XFP modules

The supported XFP module is a robust small form-factor pluggable, operating at 850nm, for up to 10 gigabits per second on SONET/SDH, Fibre Channel, Gigabit Ethernet and other applications. This module operates in single mode and multimode. Additionally, this module transmits on a 850-nanometer wavelength on Short Reach (SR), and 1310-nanometer wavelength on long reach (LR).

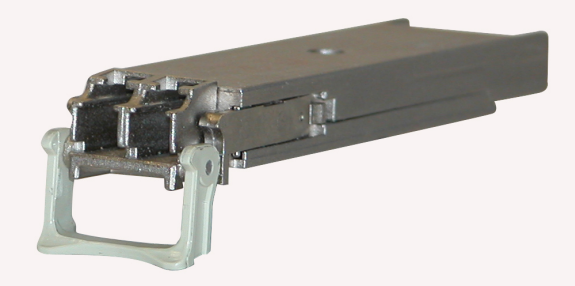

**Figure 3-5 An XFP module**

## Install a module

This section provides the steps to install a module with a bail clasp.

### Task

1 Remove the module from its protective packaging.

2 Make sure the module is the correct model for your network.

3 Locate the label on the module and make sure that the alignment groove is down.

For SFP modules, turn the module so that its label is on top. For XFP modules, turn the module so that its label is on the bottom.

4 Grip the sides of the module with your thumb and fore-finger and insert the module into the module socket.

Modules are keyed to prevent incorrect insertion.

**Figure 3-6 XFP module in a Monitoring port**

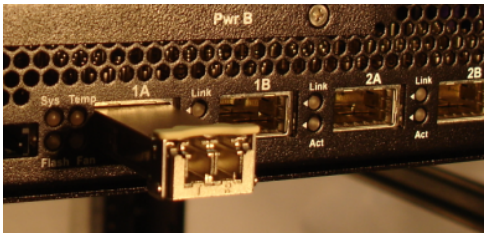


**Figure 3-7 SFP module in a Monitoring port**

## Remove a module

Perform these tasks if you need to remove an SFP or XFP module.

### Task

1. Disconnect the network fiber-optic cable from the module.
2. Release the module from the slot by pulling the bail clasp out of its locked position.
3. Slide the module out of the slot.
4. Insert the module plug into the module optical bore for protection.

# Power on the Sensor

**Before you begin**

Do not attempt to power on the Sensor until you have installed the Sensor in a rack, made all necessary network connections, and connected the power cable to the power supply.

If you are installing a redundant power supply, you should install it as described in Installing a power supply. For true redundant operation with the optional redundant power supply, McAfee recommends that you plug each supply into a different power circuit.

### Task

1. Connect the power cable to the Sensor power supply.
2. Connect the power cable to a power source.

   The Sensor has no power switch. It powers on as soon as one of its power cable is connected to a power source.

# Power off the Sensor

McAfee recommends that you use the shutdown CLI command to halt the Sensor before powering it down. For more information on CLI commands, see *McAfee Network Security Platform CLI Guide.*

4

# Attaching Cables to the Sensor

Follow the steps outlined in this chapter to connect the cables to the various ports of your Sensor.

**Contents**


- *Cable the Console port*
- *Cable the Auxiliary port*
- *Connect the cable to the Response port*
- *About the fail-open port*
- *Cable the Management port*
- *About connecting cables to the Monitoring ports*
- *Connect the cables for in-line mode*
- *Connect the cables for tap mode*
- *Connect the cables for SPAN or hub mode*
- *Cable the fail-over interconnection ports*
- *How does the fail-open function work*


## Cable the Console port

The Console port is used to set up and configure the Sensor.

**Task**

1 For console connections, plug the DB9 Console cable supplied by McAfee into the Console port.

This port is labeled **Console** on the Sensor front panel.

2 Connect the other end of the Console cable directly to a COM port of the PC or terminal server you will use to configure the Sensor, for example, a PC running the correctly configured Windows HyperTerminal software.

You must connect directly to the console for initial configuration. Required settings for HyperTerminal are:

| Name | Setting |
|---|---|
| Baud rate | 38400 |
| Number of bits | 8 |
| Parity | None |
| Stop bits | 1 |
| Flow Control | None |

3 Power on the Sensor.

# Cable the Auxiliary port

The Auxiliary port is for modem access to the Sensor for setup and configuration. You cannot use a modem the first time you configure a Sensor.

### Task

1 For modem connections, plug a straight-through modem cable into the Auxiliary port.

This port is labeled as **Aux** on the Sensor front panel.

2 Connect a modem to the **Aux** port.

3 Connect a telephone line to the modem.

Required settings for the **Aux** port are:

| Name | Setting |
|---|---|
| Baud rate | 38400 |
| Number of bits | 8 |
| Parity | None |
| Stop bits | 1 |
| Flow Control | None |

# Connect the cable to the Response port

When operating in tap or SPAN mode, the Sensor uses its Response port to respond to attacks. When deployed in tap mode, the Sensor does not inject response packets through the tap but uses the Response port.

### Task

1 Plug a Cat-5e Ethernet cable into the Response port.

This port is labeled **Rx** on the Sensor front panel.

2 Connect the other end of the cable to the network device such as a hub, switch, or a router, through which you want to respond to attacks.

# About the fail-open port

Fail-open functionality for the GE Monitoring ports is accomplished using the standard Gigabit Fail-open Bypass Kit, which is sold separately. Both copper and optical versions are available. Fail-open functionality for the 10 Gigabit Monitoring ports is accomplished using the standard 10 Gigabit (Optical) Fail-open Bypass Kit, which is also sold separately. For more information, see the documentation that accompanies the Kit.

# Cable the Management port

The Management (Mgmt) port is for communication with the Manager server.

### Task

1 Plug a Cat 5/Cat 5e Ethernet cable into the Management port.

This port is labeled **Mgmt** on the front panel of the Sensor.

2 Connect the other end of the cable to the network device, such as a hub, switch, or a router that in turn connects to the Manager server.

To isolate and protect your management traffic, McAfee strongly recommends that you use a separate, dedicated management subnet to interconnect the Sensors and the Manager.

# About connecting cables to the Monitoring ports

Connect to the network devices that you want to monitor through the Sensor monitoring ports. You can deploy Sensors in the following operating modes:

- In-line mode (fail-close)
- In-line mode (fail-open)
- External tap mode
- SPAN or hub mode
- Failover

## How to use peer ports

All full-duplex Sensor deployment modes require the use of two peer monitoring ports on the Sensor. On the Sensors, the numbered ports are wired in pairs to accommodate the traffic.

The following XFP 10 Gigabit Ethernet ports and SFP Gigabit Ethernet ports are coupled and must be used together:

| Port Pairs (and Transceiver Type) |
|---|
| 1A and 1B (XFP) |
| 2A and 2B (XFP) |
| 3A and 3B (SFP) |
| 4A and 4B (SFP) |

| Port Pairs (and Transceiver Type) |
|---|
| 5A and 5B (SFP) |
| 6A and 6B (SFP) |

You cannot configure, for example, IA and 2A to work together as a pair.

**Figure 4-1 Using peer ports**

## Default Monitoring port speed settings

Make sure that the settings on the network devices match the settings on the Sensor Monitoring ports to which they are connected.

**Table 4-1 Default Monitoring port speed settings**

| Monitoring Ports | Operating Mode | Speed/Duplex Setting |
|---|---|---|
| XFP ports<br>SFP ports | SPAN | Auto-negotiation is ON. |
| | Tap | Auto-negotiation is ON. |
| | In-line | Auto-negotiation is ON. |

## Cable types for routers, switches, hubs, and PCs

This section lists the types of cables that you require to connect the Sensor to other network devices:

- Use a crossover Ethernet RJ-45 cable to connect a router port to the 10/100/1000 copper SFP monitoring ports.
- Use a straight-through Ethernet RJ-45 cable to connect a switch or a hub port to 10/100/1000 copper SFP monitoring ports.
- Use a crossover Ethernet RJ-45 cable to connect a router port to PC to the Sensor Management port.
- Use a crossover Ethernet RJ-45 cable to connect a PC to the Sensor monitoring port.

# Connect the cables for in-line mode

The Gigabit Ethernet ports fail-close, meaning they stop the flow of traffic if the Sensor fails. To allow traffic to flow uninterrupted, you must use special hardware, and cable the Sensor to fail-open. For instructions, see the subsequent sections of this chapter.

This section provides the steps to connect the Sensor's Gigabit Ethernet ports so they fail-close.

### Task

1. Plug the cable appropriate for use with your Gigabit Ethernet into one of the Monitoring ports, for example 1A.
2. Plug another cable into the peer of the port used in Step 1.
3. Connect the other end of each cable to the network devices that you want to monitor.

   For example, if you plan to monitor traffic between a switch and a router, connect the cable connected to 1A to the switch and the one connected to 1B to the router.

## Connect the cables for tap mode

To deploy the Sensor in tap mode, you must use a Sensor's Gigabit Ethernet Monitoring port pair with a third-party external tap.

For a list of McAfee-approved third party vendors, see the KnowledgeBase at http://mysupport.mcafee.com/Eservice/. Click the link **Search the KnowledgeBase** and locate the relevant KnowledgeBase article.

### Task

1. Plug the cable appropriate for use with your Gigabit Ethernet into one of the Monitoring ports, for example, 1A.
2. Plug another cable into the peer of the port used in Step 1.
3. Connect the other end of each cable to the tap.
4. Connect the network devices that you want to monitor to the tap.

## Connect the cables for SPAN or hub mode

For the Sensor, monitoring in SPAN or hub mode occurs in in-line fail-open mode. When you monitor in SPAN or hub mode, you use only single ports.

To connect an Sensor to a SPAN port or hub, plug an LC fiber-optic or 45 cable into one of the modules and connect the other end of the cable to the SPAN port or the hub.

## Cable the fail-over interconnection ports

Fail-over requires connecting two identical M-3050/M-4050 Sensors running on the same software version using an interconnection cable or cables. Gigabit ports 2A is the interconnection port on the M-3050/M-4050. A failover cable is the only additional hardware required to support fail-over communication between two M-3050/M-4050 Sensors.

### Task

1 Plug the cable appropriate for use with your XFP module into port 2A of the active Sensor.

2 Connect the other end of the cable to port 2A of the standby Sensor.

**Figure 4-2 Sensors connected for failover**

## How does the fail-open function work

The standard Gigabit Fail-Open Kit and the 10 Gigabit Fail-Open Kit minimize the potential risks of in-line Sensor failure on critical network links. You need to purchase these kits separately. Both copper and optical versions of the kit are available for the one gigabit ports. A 10 Gigabit Optical Kit is available for the 10 gigabit ports.

The Monitoring ports of the Sensors fail-close; thus, if the Sensor is deployed in-line, a hardware failure results in network downtime. For the Monitoring ports to fail-open, you use the optional external bypass switch provided in a Fail-Open Kit.

With the bypass switch in place, normal Sensor operation supplies power to the switch through a control cable. While the Sensor is operating, the switch is "on" and routes all traffic directly through the Sensor. When the Sensor fails, the switch automatically shifts to a bypass state; in-line traffic

continues to flow through the network link but is no longer routed through the Sensor. Once the Sensor resumes normal operation, the switch returns to the "on" state, once again enabling in-line monitoring.

Sensor outage breaks the link connecting the devices on either side of the Sensor for a brief moment and requires the renegotiation of the network link between the two peer devices connected to the Sensor. Depending on the network equipment, this disruption introduced by the renegotiation of the link layer between the two peer devices might range from a couple of seconds to more than a minute with certain vendors' devices.

A very brief link disruption might also occur while the links between the Sensor and each of the peer devices are renegotiated to place the Sensor back in in-line mode. This outage, again, varies depending on the device, and can range from a few seconds to more than a minute.

You can find the installation and troubleshooting instructions for the kit in the guide that accompanies the kit. For example, for more information on the Optical kit, see the standard *Gigabit Optical Fail-Open Bypass Kit Guide.*

**See also**

*Ports* on page 10

5

# Troubleshooting the Sensor

This section lists some common installation problems, the possible causes, and the corresponding solutions.

| Problem | Possible Cause | Solution |
|---|---|---|
| LED is off. | The control cable has been disconnected. | Check the control cable and ensure it is properly connected to both the Sensor and the bypass switch. |
| LED is off. | The Sensor is powered off. | Restore Sensor power. |
| LED is off. | The Sensor port cable is disconnected. | Check the Sensor cable connections. |
| Sensor is operational but is not monitoring traffic. | Network device cables have been disconnected. | Check the cables and make sure they are properly connected to both the network devices and the bypass switch. |
| Sensor is operational but is not monitoring traffic. | The Sensor ports have not been enabled in the Manager. | The Sensor will not monitor traffic on the ports unless the ports are enabled in the Manager. Ports are disabled in case of Sensor failure; you must re-enable them for Sensor monitoring to resume. |
| Network or link problems. | Improper cabling or port configuration. | Make sure that the transmitting and receiving cables are properly connected to the Bypass Switch. |
| Runts or giants errors on switch and routers. | Improper cabling or port configuration. | Make sure that the transmitting and receiving cables are properly connected to the bypass switch. |
| The system fault "Switch absent" appears in the Manager Status page. | The control cable has been disconnected. | Check the control cable and make sure it is properly connected to both the Sensor and the bypass switch. |

6

# Sensor technical specifications

The following table lists the specifications of the Sensor:

| Sensor Specifics | Description |
|---|---|
| **Dimensions** | Without mounting ears/rails/cable management:<br>• width: 16.75 in. (41.91 cm)<br>• height: 3.5 in. (8.89 cm)<br>• depth: 30.00 in. (76.20 cm)<br>Dimensions do not include cables or power cords. |
| **Weight** | 47 lbs (21.31 kg) |
| **Voltage Range** | 100-240VAC |
| **Frequency** | 50/60Hz |
| **Vibration, operating** | Sinusoidal: 3 to 500 Hz @ 0.15 gpk<br>Random: 2.5 to 200 Hz @ 0.33 g |
| **Vibration, non-operating** | Sinusoidal: 10 to 500 Hz @ 0.8 gpk<br>Random: 2.5 to 200 Hz @ 1.05 g |
| **Power requirements** | 450W |
| **Temperature** | |
| **Ambient Temperature Range (Non-condensing)** | Operating<br>0C(32F) to 35C(95F)<br>Non-operating<br>-40C(-40F) to 70C(158F) |
| **Relative Humidity (Non-condensing)** | Operating<br>5%-90% non-condensing<br>Non-operating<br>5% to 95% non-condensing |
| **Sensor Specifics** | |

| Sensor Specifics | Description |
|---|---|
| **System Heat Dissipation** | AC (max): 535W, 1825 BTU/hr<br>DC (max): To Be determined |
| **Airflow** | 200 lfm (1 m/s) |
| **Altitude** | Sealevel to 10,000 ft (3050m) |

A

# Regulatory, compliance, and safety information

The Sensor meets the following standards:

| **Sensor regulatory, safety, and compliance** | |
|---|---|
| Regulatory: | Products with the CE Marking are compliant with the 89/336/EEC and 73/23/EEC directives, which include the safety and EMC standards listed. |
| Safety certification: | EN 55024: 1998 + A1:2001 + A2: 2003 - Immunity:<br>• EN-61000-4-2: ESD Immunity<br>• EN-61000-4-3: Radiated Immunity<br>• EN-61000-4-4 EFT/B Immunity<br>• EN-61000-4-5: Surge Protection<br>• EN-61000-4-6: Conducted Immunity<br>EN-61000-4-11: Voltage Interruption/Dips (N/A for DC)<br>CISPR/KN22 :<br>• KN-61000-4-2: ESD Immunity<br>• KN-61000-4-3: Radiated Immunity<br>• KN-61000-4-4 EFT/B Immunity<br>• KN-61000-4-5: Surge Protection<br>• KN-61000-4-6: Conducted Immunity<br>• KN-61000-4-11: Voltage Interruption/Dips (N/A for DC) |
| Electromagnetic compliance (emissions): | FCC Part 15 Class A/Industry Canada ICES-003 Issue 4, February 7, 2004 Class A<br>VCCI V-1/93.11, V-2/97.04, V-4/97 Class A<br>AS/NZS CISPR22: 2004 Class A<br>CNS 13438: May 1997<br>SS IEC CISPR22: 1993, Singapore IDA Class A<br>EN 55024: 1998 + A1:2001 + A2: 2003 - Emissions: |

| Sensor regulatory, safety, and compliance | |
|---|---|
| | • Radiated Emissions<br>• Conducted Emissions<br>• EN 61000-3-2: 2000 Harmonic Current Emissions<br>• EN 61000-3-3: 1995 + A1: 2001 Voltage Fluctuation/Flicker<br>CISPR/KN22:<br>• Radiated Emissions<br>• Conducted Emissions |

# Index


## A

about this guide 5
Auxiliary port 28

## C

Cable types for switches 30
Cabling for In-line mode 30
Cabling for SPAN 15, 31, 32
Cabling for TAP mode 31
Cabling the Console port 27
Cabling the Fail-open port 29, 30
chasis 25
conventions and icons used in this guide 5

## D

documentation
- audience for this guide 5
- product-specific, finding 6
- typographical conventions and icons 5

## F

front panel 11, 17

## H

hot swappable power supply 22

## M

Management port 29
McAfee ServicePortal, accessing 6
module 24, 25

## P

peer 29, 31
Pluggable 23
ports 10
power supply 21

## R

rack 16, 19, 20
Response port 28

## S

Safety 39
sensor responsibilities 8
ServicePortal, finding product documentation 6
setting up 19, 27
SFP 23
SFP module 25
specifications 37

## T

Technical Support, finding product information 6
Troubleshooting 7, 8, 15, 19, 35

## X

XFP module 9, 10, 24